Discrete Mathematics 33 (1981) 197–207

THE SMALLEST LENGTH OF BINARY 7-DIMENSIONAL LINEAR CODES WITH PRESCRIBED MINIMUM DISTANCE

Henk C.A. van TILBORG
Department of Mathematics, Eindhoven University of Technology, Eindhoven, The Netherlands

Received 4 December 1979
Revised 2 June 1980

Let $n(k, d)$ denote the smallest value of n for which a binary (n, k, d) code exists. Then $n(k, d)$ was known for all d, when $k \leq 6$. All values of $n(7, d)$ will now be presented.

1. Introduction

In [7] one can find a table of values of resp. bounds on the minimum distance d of an (n, k, d)-code i.e. a binary, linear, k-dimensional code of length n with minimum distance d. The first open entries in this table are at $k = 6$. In this context it is natural to define the number $n(k, d)$ as follows.

Definition 1.1. $n(k, d) := \min\{n \in \mathbb{N} \mid \text{there exists an } (n, k, d) \text{ code}\}$.

The most relevant theorems in connection with the value of $n(k, d)$ are the following.

Theorem 1.2 (Griesmer, [6]). *Let $\lceil x \rceil$ denote the smallest integer $\geq x$, then*

$$n(k, d) \geq d + n(k-1, \lceil d/2 \rceil), \tag{1.1}$$

$$n(k, d) \geq g(k, d) := \sum_{i=0}^{k-1} \lceil d/2^i \rceil. \tag{1.2}$$

Theorem 1.3 (Solomon and Stiffler, [11]). *Let $s = \lceil d/2^{k-1} \rceil$ and $s \cdot 2^{k-1} - d = \sum_{i=1}^{p} 2^{u_i - 1}$, where $k > u_1 > u_2 > \cdots > u_p > 0$. Then*

$$\sum_{i=1}^{p} u_i \leq s \cdot k \quad \Rightarrow \quad n(k, d) = g(k, d).$$

This result has been generalized to the following result.

Theorem 1.4 (Belov, [3]). *Let $s = \lceil d/2^{k-1} \rceil$ and $s \cdot 2^{k-1} - d = \sum_{i=1}^{p} 2^{u_i - 1}$, where $k > u_1 > u_2 > \cdots > u_p > 0$. If*

$$\sum_{i=1}^{\min(p, s+1)} u_i \leq s \cdot k$$

or

$$u_s - u_p = p - s, \quad \textit{and} \quad u_i \in \{1, 2\}$$

then $n(k, d) = g(k, d)$.

Later on we shall describe a code meeting the Griesmer bound (i.e. (1, 2)), whose parameters do not satisfy one of the two conditions in Theorem 1.4.

Remark 1.5. As observed in [2], it follows from Theorem 1.3 (and a fortiori from Theorem 1.4) that for fixed k and d sufficiently large $n(k, d)$ equals $g(k, d)$.

It follows from Theorem 1.2 and 1.4 together with remark 1.5 that $n(k, d) = g(k, d)$ for all pairs (k, d), $k \leq 7$ except possibly for

$$k = 5, \quad 3 \leq d \leq 6; \tag{1.3}$$

$$k = 6, \quad 3 \leq d \leq 14 \text{ and } 19 \leq d \leq 20; \tag{1.4}$$

$$k = 7, \quad 3 \leq d \leq 30, 35 \leq d \leq 44 \text{ and } 67 \leq d \leq 72. \tag{1.5}$$

Belov conjectured in [3] that his two sufficient conditions for $n(k, d) = g(k, d)$ are also necessary for $s = 1$. Strong support for his conjecture comes from the following two results.

Theorem 1.6 (Logačev, [10]). *If* $3 \leq d \leq 2^{k-2} - 2$, *then*

$$n(k, d) \geq g(k, d) + 1.$$

Theorem 1.7. (van Tilborg, [13]). *If* $2^{k-2} + 3 \leq d \leq 2^{k-2} + 2^{k-3} - 4$, *then*

$$n(k, d) \geq g(k, d) + 1.$$

Combination of these two theorems with the table in [7] yields that $n(k, d) = g(k, d) + 1$ for $k = 5$, $3 \leq d \leq 6$ and $k = 6$, $3 \leq d \leq 14$. Similarly a result in [2] shows that $n(6, d) = g(6, d) + 1$ for $19 \leq d \leq 20$, so for $k \leq 6$ all the values of $n(k, d)$ are known.

2. Some techniques

Definition 2.1. Let G be the generator matric of a binary linear code C with top row $\mathbf{c}$. Then the *residual* resp. *derived* code of C with respect to $\mathbf{c}$ (abbreviated to: w.r.t. $\mathbf{c}$) is the code generated by the restriction of G to the columns where $\mathbf{c}$ has a zero resp. a nonzero entry. We shall often denote these codes by C^0 resp. C^1 and similarly the corresponding parts of G by G^0 resp. G^1.

Lemma 2.1. *Let C be an (n, k, d) code, $\mathbf{c} \in C$ of weight w, where $\lfloor \frac{1}{2}w \rfloor < d$ and where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. Then the residual code C^0 of C w.r.t. $\mathbf{c}$ has parameters $(n - w, k - 1, d^0)$, where $d^0 \geq d - \lfloor \frac{1}{2}w \rfloor$.*

Proof. Let $\mathbf{c}' \in C$, $\mathbf{c}' \neq \mathbf{0}$, $\mathbf{c}' \neq \mathbf{c}$. Then $\mathbf{c}'$ or $\mathbf{c}'+\mathbf{c}$ has inner product $\leq \lfloor \frac{1}{2}w \rfloor$ with $\mathbf{c}$. So the restriction of $\mathbf{c}'$ to C^0 has weight $\geq d - \lfloor \frac{1}{2}w \rfloor$. □

Lemma 2.2. *Let C be an (n, k, d) code with generator matrix G. If G has two repeated columns, then shortening C on these two positions yields an $(n-2, k-1, d)$ code C^*.*

Proof. W.l.o.g. G has the form

$$\left(\begin{array}{cc|c} 1 & 1 & * \quad * \cdots\cdots * \\ \hline 0 & 0 & \\ & & \\ & & G^* \\ & & \\ 0 & 0 & \end{array}\right)$$

where G^* clearly generates the $(n-2, k-1, d)$ code C^*. □

Definition 2.3. (Farrell, [5]). An (m, k, δ) *anticode* is a k-dimensional, linear code of length m in which the maximal weight equals δ.

Lemma 2.4. (Farrell, [5]). *Let G be the generator matrix of an (n, k, d) code. By puncturing a set of columns of G, which generate an (m, k', δ) anticode, one obtains an $(n-m\ k'', d-\delta)$ code.*

On page 127 in [9] one can find the following result by MacWilliams.

Theorem 2.5. *Let C be a binary, linear code. Let A_k and B_k, $0 \leq k \leq n$, denote the number of codewords of weight k in C, resp. in its dual code. Then*

$$B_k = |C|^{-1} \sum_{i=0}^{n} A_i K_k(i), \quad 0 \leq k \leq n,$$

where

$$K_k(i) = \sum_{l=0}^{k} (-1)^l \binom{n-i}{k-l}\binom{i}{l}, \quad 0 \leq i, k \leq n.$$

Table 2.6.

$$K_0(i) = 1,$$

$$K_1(i) = n - 2i,$$

$$K_2(i) = \binom{n}{2} - 2ni + 2i^2$$

$$K_3(i) = \frac{1}{3}\left\{3\binom{n}{3} - (3n^2 - 3n + 2)i + 6ni^2 - 4i^3\right\}.$$

3. The case $k = 7$

By (1, 5) we are left with the following three gaps:

$$3 \leq k \leq 30, \qquad 35 \leq d \leq 44 \quad \text{and} \quad 67 \leq d \leq 72.$$

Since $n(k, 2e+2) = 1 + n(k, 2e+1)$ it is sufficient to consider only even values of d.

The following values of $n(k, d)$ follow from the table in [7].

$$n(7,4) = 12, \qquad n(7,12) = 27,$$
$$n(7,6) = 16, \qquad n(7,24) = 50.$$
$$n(7,8) = 19,$$

Comparing [7] with Theorem 1.6 (i.e. [10]) yields

$$n(7,30) = 62.$$

Since the appearance of [7] several improvements have been made to its table. The following references in combination with Theorems 1.6 and 1.7 lead to new values of $n(k, d)$:

Alltop [1]: $n(7,42) = 87$, $n(7,44) = 90$,

Farrell [5]: $n(7,36) = 75$, $n(7,38) = 79$, $n(7,40) = 82$,

Van Tilborg [12]: $n(7,20) = 43$.

Farrell describes his codes by means of anticodes (see Definition 2.3). A different description of these codes is by the following generator matrix:

$$G = \left(\begin{array}{c|c} \overset{\leftarrow 64 \rightarrow}{1\ 1\ 1 \cdots 1} & 0\ 0 \cdots 0 \\ \hline G_1 & G_2 \end{array}\right),$$

where the left hand side of G generates the first order Reed-Muller code of length 64 (and minimum distance), and G_2 generates a (11, 6, 4), (15, 6, 6), resp. a (18, 6, 8) code.

We shall now treat the remaining cases.

Theorem 3.1. $n(7, 10) = 24$.

Proof. According to Chen ([4]) the cyclic code C with parity check polynomial $h(x) = 1 + x^4 + x^5 + x^7 + x^8$ has parameters (51, 8, 24). Let C^0 be the residual code of C w.r.t. the minimum weight code word $g(x) = (x^{51} - 1)/h(x)$. According to Lemma 2.1 C^0 has parameters (27, 7, 12). It is not difficult to check that the 1st,

10th and 17th coordinate of C^0 from a $(3, 2, 2)$ anticode. The other 24 columns generate a $(24, k'', 10)$ code by Lemma 2.4. It is easy to verify that k'' is indeed 7, which proves that a $(24, 7, 10)$ code exists. Since $n(7, 10) \geq 24$ by Theorem 1.6 it follows that $n(7, 10) = 24$. The generator matrix of the code described above is given by

$$\left(\begin{array}{c|cccccccccccccccccccccccc}
 & 1 & 1 & & 1 & 1 & & 1 & & 1 & 1 & & 1 & 1 & & & 1 & & & & & & & \\
1 & 1 & & 1 & & 1 & 1 & 1 & 1 & 1 & 1 & & 1 & 1 & & 1 & 1 & & & & & & & \\
 & 1 & & 1 & & & & 1 & 1 & 1 & 1 & & 1 & & & 1 & 1 & 1 & 1 & 1 & & & & \\
 & & 1 & 1 & 1 & 1 & & 1 & 1 & & 1 & & 1 & & & 1 & & 1 & 1 & 1 & & & & \\
 & & & 1 & & & 1 & & 1 & & 1 & 1 & 1 & & & & & & 1 & 1 & 1 & & & \\
 & 1 & & & 1 & & & 1 & & 1 & 1 & & 1 & & & 1 & & & & & 1 & 1 & 1 & \\
 & & & & 1 & 1 & & 1 & 1 & 1 & & & 1 & & & 1 & 1 & & & & & 1 & 1 & 1
\end{array}\right)$$

□

Theorem 3.2. $n(7, 14) = 32$.

Proof. It follows from Theorem 1.6 that $n(7.14) \geq 31$. In [12] van Tilborg constructs a $(35, 7, 16)$ code, whose generator matrix consists of circulants of size 7, whose top rows correspond to $1, 1+x, 1+x^2+x^4, 1+x+x^2+x^3+x^4$ and $1+x+x^2+x^4+x^5$. Obviously the columns 1, 2 and 9 generate a $(3, 2, 2)$ anticode. It is again easy to check that the remaining columns generate a $(32, k'', 14)$ code, with $k'' = 7$. This proves that $n(7, 14) \leq 32$. We shall now prove that $n(7, 14) = 32$.

Let us assume that a $(31, 7, 24)$ code C exists. Let A_i, B_i, $0 \leq i \leq 31$ denote the weight enumerator of C resp. its dual code.

Let $\mathbf{c} \in C$ be of weight w. By Lemma 2.1 the residual code of C *w.r.t.* $\mathbf{c}$ generates a

$$(31-w, 6, 14-\lfloor \tfrac{1}{2}w \rfloor) \tag{3.1}$$

code if $w \leq 27$.

For certain values of w this is impossible by Theorems 1.2 or 1.5. In this way one proves that

$$A_w = 0 \quad \text{for } w \in \{15, 17, 18, 19, 21, 22, 23, 25, 26, 27\}. \tag{3.2}$$

By adding a codeword of weight 29 or 31 to a minimal weight codeword one would get a codeword of weight 15, 17 or 19, contradicting (3.1) or (3.2). Hence

$$A_{29} = A_{31} = 0. \tag{3.3}$$

Clearly $A_0 = B_0 = 1$ and $B_1 = 0$. It follows from Lemma 2.2 and Theorem 1.6 that C cannot have repeated columns i.e. $B_2 = 0$. Theorem 2.5 now gives rise to the 3 equations, $(k = 0, 1, 2)$, which can be rewritten as

$$A_{20} + A_{16} + A_{20} + A_{24} + A_{28} + A_{30} = 127, \tag{3.4}$$

$$A_{16} + 3A_{20} + 5A_{24} + 7A_{28} + 8A_{30} = 103, \tag{3.5}$$

$$3A_{20} + 10A_{24} + 21A_{28} + 28A_{30} = 84. \tag{3.6}$$

If $A_{30} \neq 0$, then the minimum distance of C implies that $A_{30} = 1$, $A_{20} = A_{24} = A_{28} = 0$, which contradicts (3, 6). So

$$A_{30} = 0. \tag{3.7}$$

It now follows from (3.6) that $3 \mid A_{24}$. However, two codewords of weight 24 must have inner product 17 by the minimum distance of C. So the sum of 3 codewords of weight 24 must have weight $31 - 3(24 - 17) = 10$, which is less than the minimum distance of C. So

$$A_{24} = 0. \tag{3.8}$$

It follows from the minimum distance of C that $A_{28} \leq 1$. So in view of (3.4)-(3.8) we have two possible weight enumerators for C:

(i) $A_0 = 1, A_{14} = 80, A_{16} = 19, A_{20} = 28, A_{28} = 0$,

(ii) $A_0 = 1, A_{14} = 72, A_{16} = 33, A_{20} = 21, A_{28} = 1$.

If two codewords of weight 20 have inner product 13, i.e. add up to a weight 14 codeword $\mathbf{c}$, then the residual code C^0 of C w.r.t. $\mathbf{c}$ has parameters (17, 6, 7) and contains a codeword of weight 13. The residual code of C^0 w.r.t. this weight 13 word would have parameters (4, 5, 1), which is clearly impossible.

So two codewords of weight 20 intersect in ten or twelve positions (i.e. add up to a weight 16 or 20 codeword). Suppose that two codewords of weight 20 intersect in ten positions. W.l.o.g. we have the following picture:

$$\left(\begin{array}{c|c|c|c} \longleftarrow 10 \longrightarrow & \longleftarrow 10 \longrightarrow & \longleftarrow 10 \longrightarrow & \leftarrow 1 \rightarrow \\ 1\,1\,1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 0 \\ 1\,1\,1\,1\,1\,1\,1\,1\,1\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,1\,1\,1\,1\,1\,1\,1\,1\,1 & 0 \\ a & b & c & d \end{array}\right)$$

Let a, b, c, d be the number of ones of a third codeword of weight 20 on the various sets of coordinates, as depicted above. In view of the preceding we have the following relations:

$$a + b \in \{10, 12\}, \qquad a + c \in \{10, 12\}, \qquad b + c \in \{10, 12\}.$$

So $a + b + c \leq 18$ i.e. $d \geq 2$, a contradiction.

We conclude that all codewords of weight 20 have inner product 12. Let C^0 be the residual code of C w.r.t. a weight 20 codeword. C^0 has parameters (11, 6, 4). All the other codewords of weight 20 in C have a restriction of weight 8 to C^0 by the observations made above. Since the number of weight 8 vectors of length 11 and distance at least 4 is at most 17 (see [9, appendix A, Section 2]), we have that $A_{20} \leq 1 + 17 = 18$. This contradicts (i) and (ii). We conclude that a (31, 7, 14) cannot exist, so $n(7, 14) = 32$.

Theorem 3.3. $n(7, 15) = 35$.

Proof. It follows from Theorem 1.6 that $n(7, 16) \geq 34$, while the construction of a (35, 7, 16) code in van Tilborg [12] implies that $n(7, 16) \leq 35$. Let us assume that

a (34, 7, 16) code C exists. For any $\mathbf{c} \in C$, $17 \leq w(\mathbf{c}) \leq 31$, the residual code of C w.r.t. $\mathbf{c}$ would have parameters contradicting Theorems 1.2 or 1.6. So

$$A_i = 0, \quad 17 \leq i \leq 31, \tag{3.9}$$

where A_i again denotes the weight enumerator of C. The sum of a weight 16 codeword and a weight 33 or 34 codeword would have weight 17, 18 or 19, contradicting (3, 9). So

$$A_{33} = A_{34} = 0. \tag{3.10}$$

Since C cannot have an all zero column in its generator matrix it follows that $B_1 = 0$. Since $B_0 = A_0 = 1$ Theorem 2.5 with $k = 0, 1$ reduces to

$$A_{16} + A_{32} = 127,$$
$$2A_{16} + 30A_{32} = -34,$$

i.e. $A_0 = 1$, $A_{16} = 118$, $A_{32} = 9$. However, $A_{32} \leq 1$ from the minimum distance of C. So a (34, 7, 16) code cannot exist and $n(7, 16) = 15$. □

Theorem 3.4. $n(7, 18) = 40$.

Proof. It follows from theorem 1.6 that $n(7, 18) \geq 40$. In van Tilborg [12] one can find the construction of a (42, 7, 19) code whose generator matrix consists of six circulants of size 7 with top rows corresponding to 1, $1+x$, $1+x^2+x^3$, $1+x^2+x^4$, $1+x+x^2+x^3+x^4$ and $1+x+x^2+x^4+x^5$. As at the beginning of the proof of Theorem 3.2 one easily verifies that puncturing columns 1, 2 and 9 yields a (39, 7, 17) code. The extended code of this code has parameters (40, 7, 18). So $n(7, 18) = 40$. □

Theorem 3.5. $n(7, 22) = 47$.

Proof. Again we use Theorem 1.6 and get that $n(7, 22) \geq 47$. We shall now construct a (47, 7, 22) code. As in Theorem 3.1 we start with the cyclic (51, 3, 24) code with parity check polynomial $h(x) = 1+x^4+x^5+x^7+x^8$. Deleting the first row and column of the generator matrix (with rows corresponding to $x^i(x^n - 1)/h(x)$, $0 \leq i \leq 7$) yields a (50, 7, 24) code. Deleting the columns 1, 9 and 21 (which form a (3, 2, 2) anticode) gives a (47, 7, 22) code. So $n(7, 22) = 47$. □

Theorem 3.6. $n(7, 26) = 56$.

Proof. By Theorem 1.6 one has that $n(7, 26) \geq 55$. In [1] Alltop constructs a (56, 7, 26) code so $n(7, 26) \leq 56$. So we have to prove the nonexistence of a (55, 7, 26) code. Since the proof of this result is very lengthy and involves a lot of adhoc arguments, we omit it here and refer the reader to [14]. □

Theorem 3.7. $n(7, 28) = 59$.

Proof. By Theorem 1.6 we know that $n(7, 28) \geq 58$. Let us assume that a $(58, 7, 28)$ code (exists with weight enumerator A_i, $0 \leq i \leq 58$ (and B_i for its dual code). It follows from Lemma 2.1 and Theorems 1.2 or 1.6 that

$$A_i = 0 \text{ for } 29 \leq i \leq 31,\ 33 \leq i \leq 39 \text{ and } 41 \leq i \leq 55. \tag{3.11}$$

Since the sum of a weight 28 code word and a code word of weight 57 or 58 has weight 29, 30, 31, it follows from (3.11) that

$$A_{57} = A_{58} = 0. \tag{3.12}$$

If we now apply Theorem 2.5 with $k = 0, 1, 2$ we get three equations, which can be reduced to

$$A_{28} + A_{32} + A_{40} + A_{56} = 127, \tag{3.13}$$

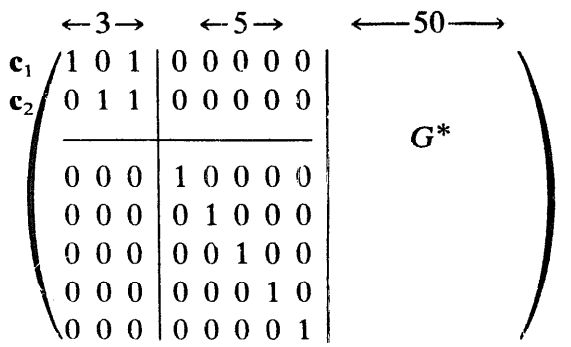
$$A_{32} + 3A_{40} + 7A_{56} = 39, \tag{3.14}$$

$$A_{40} + 7A_{56} = 6 + \tfrac{2}{3}B_2. \tag{3.15}$$

If C has repeated columns we can apply Lemma 2.2. We obtain a $(56, 6, 28)$ code. If this code again has repeated columns one would have a $(54, 5, 28)$ code, contradicting Theorem 1.2. So $B_2 \leq 1$. It follows from (3.15) that $3 \mid B_2$. So $B_2 = 0$. Now (3.15) yields that $A_{56} = 0$ and $A_{40} = 6$. With (3.13) and (3.14) we can now determine the weight enumerator of C:

$$A_0 = 1, \quad A_{28} = 100, \quad A_{32} = 21, \quad A_{40} = 6.$$

Although it is possible to give a direct proof that a code with these parameters does not exist, we shall give a different proof, which makes use of Lemma 2.4 and Theorem 3.6. We first compute B_3 with Theorem 2.5. It turns out that $B_3 = 166$. Let $\mathbf{c} \in C^{\perp}$ be of weight 3. The corresponding three columns in G of C generate a $(3, 2, 2)$ anticode, the other 55 columns generate a $(55, k'', 26)$ code by Theorem 3.6. W.l.o.g. G has the following form



Since $\mathbf{c}_1$ and $\mathbf{c}_2$ must have weight 28 or 32 and have distance at least 28, it is easy to check that the last 55 columns have rank 7, i.e. the restriction of G to the last 55 coordinates generates a $(55, 7, 26)$ code. This contradicts Theorem 3.6. We

conclude that $n(7,28) \geq 59$. In [5] Farrell claims the existence of a $(59,7,28)$ code. However, the construction described there uses an anticode which has repeated columns, while it should not have repeated columns. Luckily Dr. T. Helleseth helped us in finding a $(59,7,28)$ code. It is a matter of straightforward checking that the following matrix generates a $(59,7,28)$ code, thus proving that $n(7,28) = 59$.

$$G = \begin{pmatrix}
11111111111111111111111111111111111111111111110000000 \\
11111111111111111111111000000000000000000000001000001 \\
11111111111100000000000111111111111000000000000100001 \\
11111100000011111100000011111100000011111100000010001 \\
11110001110001110001110001110001110001110001111000001001 \\
11001101101001101001001100110100100110010011001100000101 \\
10101011010101001100101010100010110101011010101010100000011
\end{pmatrix}$$

The weight enumerator of this code is given by $A_0 = 1$, $A_{28} = 78$, $A_{32} = 47$, $A_{36} = 1$, $A_{52} = 1$.

Theorem 3.8. $n(7,68) = 138$, $n(7,70) = 142$, $n(7,72) = 145$.

Proof. It follows from the Griesmer bound that $n(7,68) \geq 138$, $n(7,70) \geq 142$ and $n(7,72) \geq 145$. In [8] one can find the following $(145,7,72)$ code.

$$G = \left(\begin{array}{c|c|c}
\overleftarrow{49} & \overleftarrow{\quad 64 \quad} & \overleftarrow{32} \\
 & 1\ 1\ 1 \cdots\cdots 1 & 0 \cdots\cdots 0 \\
 & & 1 \cdots\cdots 1 \\
G_1 & G_2 & G_3
\end{array}\right)$$

where the middle sixty four and the last thirty two columns generate the 1st order Reed-Muller code of length 64 resp. 32 and where G_1 is the following matrix

$$\begin{pmatrix}
11111111111111111111111100000000000000000000000000^{**}0000000^{*} \\
11111111111111110000000000000000000000000000000000000000 \\
11111111000000001111111111111111111111110000000000 \\
11111100111111001111000011111111110000000111111000 \\
11110011111100111100110011111100001111001111001 10 \\
11001111110011111010101011110011001100111101010 1 \\
10101010101010101111111111001010101010101011011111 1
\end{pmatrix}$$

This code has weight enumerator

$$A_0 = 1, \quad A_{72} = 111, \quad A_{80} = 15, \quad A_{88} = 1.$$

So $n(7,72) = 145$. It is rather trivial to verify that puncturing the columns

indicated by an * (these three form a (3, 2, 2) anticode) yields a (142, 7, 70) code. Moreover the last 32 columns clearly contain a set of four columns which together with the three columns from above, form a (7, 3, 4) anticode. Puncturing these seven coordinates yields a (138, 7, 68) code (note that the middle segment of G is still completely present and has full rank). So $n(7, 70) = 142$ and $n(7, 68) = 138$.

The following Table 1 shows the values of $n(7, d)$ which are not covered by Belov. In other words for values of d which are not listed one has that

$$n(7, d) = \sum_{i=0}^{d-1} \lceil d/2^i \rceil.$$

Table 1. Values of $n(7, d)$ not covered by Belov [4]

d	$n(7, d)$	comment
4	12	by Helgert & Stinaff [7]
6	16	by Helgert & Stinaff [7]
8	19	by Helgert & Stinaff [7]
10	24	by Theorem 3.1
12	27	by Helgert & Stinaff [7]
14	32	by Theorem 3.2
16	35	by Theorem 3.3
18	40	by Theorem 3.4
20	43	by Helgert & Stinaff and van Tilborg [7, 12]
22	47	by Theorem 3.5
24	50	by Helgert & Stinaff [7]
26	56	by Theorem 3.6
28	59	by Theorem 3.7
30	62	by Helgert & Stinaff and Logačev [7, 10]
36	75	by Farrell and van Tilborg [5, 13]
38	79	by Farrell and van Tilborg [5, 13]
40	82	by Farrell and van Tilborg [5, 13]
42	87	by Alltop and van Tilborg [1, 13]
44	90	by Alltop and van Tilborg [1, 13]
68	138	by Theorem 3.8
70	142	by Theorem 3.8
72	145	by Theorem 3.8

Remark. The codes described in Theorem 3.8 are the only known linear codes meeting the Griesmer bound, which do not follow from one of the two constructions in Belov's theorem. This means that his conjecture, stated for $s = 1$, is certainly not true for $s > 1$.

References

[1] W.O. Alltop, Binary codes with improved minimum weights, IEEE Trans. Inform. Theory, IT 22 (1976) 241–243.

[2] L.O. Baumert and R.J. McEliece, A note on the Griesmer bound, IEEE Trans. Inform. Theory, IT 19 (1973) 134–135.

[3] B.I. Belov, A conjecture on the Griesmer bound, Optimization methods and their applications (All-Union Summer Sem., Khakusy, Lake Baikal, 1972) (Russian), 100–106, 182. Sibirsk. Energet. Inst. Sibirsk, Otdel, Akad. Nauk SSR, Irkutsk, 1974.

[4] C.L. Chen, Computer results on the minimum distance of some binary cyclic codes, IEEE Trans. Inform. Theory, IT-16 (1970) 359–360.

[5] P.G. Farrell, An introduction to anticodes, CISM Summer School: Algebraic coding theory and applications, 1978.

[6] J.H. Griesmer, A bound for error-correcting codes, IBM J. Res. Develop. 4 (1960) 532–542.

[7] H.J. Helgert and R.D. Stinaff, Minimum distance bounds for binary linear codes, IEEE Trans. Inform. Theory 19 (1973) 344–356.

[8] T. Helleseth and H.C.A. van Tilborg, A new class of codes meeting the Griesmer bound, to appear.

[9] F.J. MacWilliams and N.J.A. Sloane, The theory of Error Correcting Codes, North Holland Mathematical Library, Vol. 16 (North Holland, Amsterdam, 1977).

[10] V.W. Logačev, An improvement of the Griesmer bound in the case of small code distances, Optimization methods and their applications (All-Union Summer Sem., Khakusy, Lake Baikal, 1972) (Russian), 107–111, 182 Silbirsk. Energetic. Inst. Sibirsk. Otdel. Akad. Nauk SSSR, Irkutsk, 1974.

[11] G. Solomon and J.J. Stiffler, Algebraically punctures cyclic codes, Inform. and Control 8 (1965) 170–179.

[12] H.C.A. van Tilborg, On quasi-cyclic codes with rate $1/m$, IEEE Trans. Inform. Theory, IT-24 (1978) 628–630.

[13] H.C.A. van Tilborg, On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound, Inform. and Control 44 (1980) 16–35.

[14] H.C.A. van Tilborg, a proof of the nonexistence of a binary (55, 7, 26) code, Technological University of Eindhoven, TH-Report 79-WSK-09.